PREVENTING UNAUTHORIZED SWITCHING OF MOBILE TELECOMMUNICATIONS SERVICE PROVIDERS

TECHNICAL FIELD

[0001] The present invention is directed to the field of telecommunications and, more particularly, to security in the field of telephone number portability.

BACKGROUND

[0002] As the popularity of network communications increases, more and more communications service providers are offering their services to potential subscribers. A person wishing to purchase and use a wireless device (e.g., mobile phone, PDA, etc.) often is forced to choose among several service providers that offer various services and products. Once a subscriber selects a particular service provider, competitors may attempt to lure the subscriber away from her selected service provider by offering lower prices, more network time, free devices/features, etc. In the past, many subscribers balked at switching service providers because switching service providers also typically meant switching phone numbers, resulting in inconvenience to the subscriber.

[0003] However, with the advent of industry-wide number portability, subscribers of mobile communications services are allowed to retain a particular phone number while switching service providers and/or service regions. For example, a subscriber currently with Carrier A can keep her phone number even after switching to Carrier B's services.

[0004] Number portability is not free of problems, however. Because switching service providers becomes more or less invisible to the subscriber when the

subscriber's phone number stays the same, there is an increased likelihood that unethical service providers or other unethical parties may attempt fraudulent and unauthorized switching, thereby harming unsuspecting subscribers.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Figure 1 is a block diagram of a suitable system for practicing embodiments of the invention, including preventing unauthorized switching of mobile telecommunications service providers.

[0006] Figure 2 is a flow diagram showing an example of communication data between a mobile customer and first and second mobile communications service providers.

[0007] Figure 3 is a flow diagram showing an example of communication data between a mobile customer, a third party porting administrator, and first and second mobile communications service providers.

[0008] Figure 4 is a flow diagram of an example routine for setting up a user account with a new portable phone number and unauthorized port protection.

[0009] Figure 5 is a flow diagram of an example routine for associating a portable phone number with an interchangeable routable number and a user password for implementing unauthorized port protection.

[0010] Figure 6 is a flow diagram of an example routine for switching mobile communications service providers given an existing portable phone number that is protected from unauthorized porting.

[0011] Figure 7 is a flow diagram of an example routine for associating a portable phone number with a new interchangeable routable number when the portable phone number is protected from unauthorized porting in accordance with one embodiment of the invention.

[0012] Figure 8 is a flow diagram of an example routine for authorizing a port request for a portable phone number that is protected from unauthorized porting.

[0013] Figure 9 is a flow diagram of an example routine for obtaining authorization from a customer wishing to switch service providers when unauthorized port protection is in place.

[0014] The headings provided herein are for convenience only and do not necessarily affect the scope or meaning of the claimed invention.

[0015] In the drawings, the same reference numbers identify identical or substantially similar elements or acts. To easily identify the discussion of any particular element or act, the most significant digit or digits in a reference number refer to the figure number in which that element is first introduced (e.g., block 302 is first introduced and discussed with respect to Figure 3).

DETAILED DESCRIPTION

[0016] Described in detail below are systems and associated methods for providing protection from unauthorized switching of mobile communications service providers in a communications network configured for number portability. The systems and associated methods provide a mobile customer, such as a mobile device user or an employer, parent, etc., of a mobile device user, with protection against having the portable phone number associated with an unauthorized service provider.

[0017] A portable phone number is one that can be enduringly associated with a particular mobile customer, even when that mobile customer switches mobile communications service providers. The process of switching service providers is sometimes called "porting." Using the techniques described herein, as well as similar techniques and variations, a customer is protected from unauthorized switching of service providers, even though the assigned portable phone number is otherwise easily switched or "ported" from one service provider to another.

[0018] In one embodiment of the invention, a portable phone number is linked to a selected service provider by associating the portable phone number with a second number, such as a network routing number or a device identification number (herein generally referred to as a "routable number"), which is unique to and

compatible with the selected service provider's network. In this way, when a call is made by dialing the portable phone number, the portable phone number can be used to identify the routable number, which can then be used to route the call to the appropriate device.

[0019] At least one data store, accessible by multiple communications service providers, may be used to store the association between the phone number and the routable number. When a call is made, the routable number can be looked up in the data store at a switching point. When the customer wants to change service providers but keep the same phone number, the data store is modified so that the customer's portable phone number is associated with a new routable number that is compatible with a new service provider's network.

[0020] Because the porting process is relatively simple and is invisible to the customer, portable phone numbers are prone to misuse by unethical parties hoping to profit by switching a customer's service provider without the customer's knowledge. To prevent unauthorized switching of service providers, the disclosed system and method permits various techniques to prevent altering the association between a portable phone number and a routable number without the customer's authorization. Some of these techniques rely on limiting writable access to the data store that stores the association between phone number and routable number. For example, a third party administrator may exclusively control writable access to the data store. In such a case, the third party will revise the association between the portable phone number and the routable number only when given the proper assurance that the customer, either directly or indirectly, has authorized the change.

[0021] In another example, a current service provider may be given limited writable access to a shared data store, but only with respect to the portions of the data store pertaining to its own customers or any new customers that have not yet been assigned a portable phone number. Then, when provided with acceptable customer authorization, the current service provider can revise the information in the data store so the customer's portable phone number is associated with a new

routable number that is compatible with and unique to the network of a newly selected service provider. Alternatively, the current service provider can transfer writable access permission from itself to the newly selected service provider, so the newly selected service provider can modify the data store as necessary to complete the switch.

[0022] In the case where a password (or similar authorization information) is used for authorization, either the current service provider or a third party administrator stores an association between a customer and that customer's password. In this way, a request for switching the customer's service provider can be authorized by receiving the password and verifying that it is associated with the relevant customer. In addition to passwords, other authorization information, such as biometrics, voice signatures, etc., may be used.

[0023] In an alternative technique that does not involve passwords or similar authorization techniques such as those described above, authorization may be based on the occurrence of some event. For example, a customer can authorize a switch by replying to a voice- or text-message sent to her on her mobile communications device. In another example, a customer can authorize a switch by dialing into a special number using her mobile communications device. In yet another example, a new service request placed electronically by a customer may be logged in a system configured to provide automated authorization information to the necessary parties/systems.

[0024] The invention will now be described with respect to various embodiments. The following description provides specific details for a thorough understanding of, and enabling description for, these embodiments of the invention. However, one skilled in the art will understand that the invention may be practiced without these details. In other instances, well-known structures and functions have not been shown or described in detail to avoid unnecessarily obscuring the description of the embodiments of the invention.

[0025] The terminology used in the description presented below is intended to be interpreted in its broadest reasonable manner, even though it is being used in

conjunction with a detailed description of certain specific embodiments of the invention. Certain terms may even be emphasized below; however, any terminology intended to be interpreted in any restricted manner will be overtly and specifically defined as such in this Detailed Description section.

I. Representative System

[0026] Figure 1 is a block diagram of a suitable system for practicing embodiments of the invention, including preventing unauthorized switching of mobile telecommunications service providers. For clarity, portions of the system that are well known in the art, such as various base stations and switches, etc., are not shown in Figure 1.

[0027] The system includes a device 102, such as a mobile phone, PDA, etc., having a portable number (e.g., MIN, MSISDN, etc.). The device 102 is associated with a selected service provider subsystem 104, including a home location register 106 and a customer care/billing center 108. The customer care/billing center 108 has access to a number portability database 110, either directly or through a portability administrative center 112. The number portability database 110 stores an association between the portable number associated with the device 102 and a routable number (e.g., MDN, SIM, ICCID, IMSI, etc.), such as a mobile identification number or routing number that is unique to and compatible with the selected service provider subsystem 104.

[0028] Various parties may have permission to update the database. If the service provider 104 has only indirect access for writing to the number portability database 110, changes to the database are made via requests to the portability administrative center 112. If, however, the service provider 104 has direct access to write to the number portability database 110, changes may be made directly by, for example, an administrator at the customer care billing center 108. However, such directed writable access may be limited (e.g., the service provider system may only be able to write to the database with respect to its own customers).

[0029] In some embodiments, the number portability database 110 is shared between multiple service providers, meaning it (1) stores customer information for

multiple service providers and (2) is accessible by system components of multiple service providers so it can be used to route calls made to ported numbers regardless of service provider. For example, a calling device 114 can place a call to the device 102 by dialing the portable phone number. The call is routed through a switching center 116 to a signal transfer point 118, where the number portability database 110 is checked for information about the portable number, including the associated routable number. Once the routable number associated with the portable phone number is identified, the home location register 106 associated with the device 102 can be checked for further information about the location of the device 102. When the necessary information is known, the call can be routed to the device 102 via a telecommunications network 120, such as a public switched telephone network, packet switched network, combination/hybrid network, etc.

II. Representative Flows

[0030] Referring to Figures 2 and 3, representative message or data flow diagrams depict exchanges of communications between a customer desiring service for one or more mobile devices, a first service provider subsystem, a second service provider subsystem, and (optionally) a third party portability administrator, such as the portability administrative center 112 of Figure 1. These and other flow diagrams do not show all functions or exchanges of data, but instead they provide an understanding of commands and data exchanged under the system. Those skilled in the relevant art will recognize that some functions or exchange of commands and data may be repeated, varied, omitted, or supplemented, and other (less important) aspects not shown may be readily implemented.

[0031] Figure 2 is a flow diagram showing an example of communication data between a mobile customer 202, a first wireless service provider 204, and a second wireless service provider 206. In communication 208, the customer 202 requests new service from the first service provider 204. Based on this request, the first service provider 204 assigns a portable phone number and a routable

number to the customer 202. The portable phone number is unique to the customer 202 and is the number that callers will dial when they want to call the customer's mobile device. The routable number is compatible with and unique to the communication network of the first service provider 204 and, in some cases, may be unique to the wireless device of the customer.

[0032] Once the portable phone number and the routable number are assigned to the customer 202, the first service provider 204 registers a mapping between the portable phone number and the routable number in a portable number database, such as the number portability database 110 of Figure 1, that is accessible by multiple communications service providers within a communications network. In communication 210, the first service provider 204 offers unauthorized port protection to the customer 202 to protect the customer 202 from having the service provider switched without the customer's authorization. In communication 212, the customer 202 accepts the offer for unauthorized port protection. Because some embodiments rely on passwords for authorization processes, acceptance of the offer for unauthorized port protection may involve the customer 202 providing a password that can be used to authorize a port request when switching of service providers is desired. The first service provider 204 then stores a record of this password in association with the customer 202 and activates service so the customer 202 can then proceed with use of the mobile device without having to worry about an unauthorized switching of service provider.

[0033] In communication 214, the user has decided to switch service providers but retain the same portable phone number and sends a request for new service to the second service provider 206. In communication 216, the customer 202 authorizes porting of the portable phone number by providing a password to the first wireless service provider 204 indicating that the port is authorized. Alternatively, this password may be provided to the first service provider 204 indirectly. For example, the customer 202 may provide the password to the

second service provider 206 who then passes it on to the first service provider 204 as part of a port request.

[0034] After receiving the request for new service from the customer 202 (communication 214), the second service provider 206, in communication 218, sends a wireless port request to the first service provider 204 so the customer 202 can switch from the first service provider 204 to the second service provider 206. After receiving the port authorization of communication 216, the first service provider 204 verifies the port request and sends an accept port request communication 220 to the second service provider 206. The second service provider 206 then assigns to the customer's 202 device a new routable number that is compatible with and unique to the second service provider's 206 network. This new routable number will then be mapped to the customer's 202 portable phone number and registered in the number portability database, such as the database 110 of Figure 1. The customer 202 can then request unauthorized port protection via the second wireless provider 206.

[0035] Figure 3 is a flow diagram showing an example of communication data between a mobile customer 202, a first wireless service provider 204, a second wireless service provider 206, and a third party porting administrator 308. In this example, the third party porting administrator 308 handles database information that includes mapping between a customer's portable phone number and the customer's current routable number.

[0036] In communication 310 the customer 202 requests a subscription for service from the first wireless service provider 204. In some embodiments, as shown in Figure 3, this request is handled by the third party porting administrator 308 on behalf of the first service provider 204. Based on this request, the third party porting administrator 308 assigns a portable phone number and a routable number compatible with and unique to the first service provider's 204 network. To ensure that the assigned identification number is compatible with and unique to the first service provider's 204 network, the third party porting administrator 304 may need to identify a suitable routable number by requesting one from the first

service provider 204 or, alternatively, identify a number from an available number database. Once the portable phone number and the routable number are assigned, the third party porting administrator 308 stores the portable phone number and the routable number in a database that is accessible by multiple wireless providers. Information relating to the association between the two numbers is also stored in the database, sometimes called a "mapping."

[0037] In communication 312, the third party porting administrator 308 offers unauthorized port protection to the customer 202. In communication 314 the customer 202 accepts the offer for unauthorized port protection and, if the authorization technique utilizes a password, provides a password to the third party porting administrator 308. The third party porting administrator 308 stores a password record in association with the customer 202 so the customer 202 can later authorize switching of wireless service providers using the password. As an alternative to password authorization, other authorization techniques, such as a response to a notification message or a call to a designated authorization number, may be utilized.

[0038] In communication 316 the third party porting administrator 308 sends a notification to the first service provider 204 that the portable phone number and routable number have been assigned to the customer 202. Accordingly, the first service provider 204 can begin offering service to the customer 202. Based on this service, the customer 202 can be called using the portable phone number.

[0039] In communication 318 the customer 202, wishing to switch service providers, provides a port authorization and service switch request to the third party porting administrator 308. In an alternate embodiment (not shown), the customer 202 may request service from the second service provider 206, who then provides a request to the third party porting administrator 308. Based on the switch service request, the third party porting administrator 308 assigns a new routable number that is compatible with and unique to the second wireless service provider's 206 network. The customer 202 keeps the original portable phone number. The third party porting administrator 308 then stores the new portable

phone number/identification number combination in its database. In communication 320 the third party porting administrator 308 sends a registration complete message to the second service provider 206 and the first service provider 204, so the appropriate services can be terminated and initiated.

[0040] In some embodiments, notifications 316 and 320 may be conditional and based on acceptance by the selected service provider. In this way, the service provider can, for example, check the customer's credit history, etc. In an alternate embodiment, new service requests, such as those of communications 310 and 318, may be provided by the respective service providers rather than by the customers. Additionally, passwords and other authorization information may be provided to the third party porting administrator 308 indirectly, via the wireless service providers 204 and 206.

[0041] Referring to Figures 4 through 9, some functionality performed by the system of one embodiment of the present invention is shown as one or more routines. These routines may be hardware-based, embodied in software in a computer-readable medium, or any combination of the two.

[0042] Figure 4 is a flow diagram 400 of an example routine for setting up a customer account subscription for a new portable mobile phone number, including unauthorized port protection. This routine can be performed, for example, at a communications service provider or, alternatively, at a third party portable administration center, such as the portability administration center 112 of Figure 1. In block 401, the routine receives a customer request for new mobile phone service. In block 402, the routine assigns a new portable phone number and a routable number to the customer (having one or more devices). In decision block 403, the routine determines whether the customer desires unauthorized port protection by querying the customer. If the routine determines that the customer does not desire unauthorized port protection, the routine continues at block 405. However, if the routine determines that the customer desires unauthorized port protection, the routine continues at block 404, where the routine stores a customer password for the customer account so future modifications of service providers

can be authorized when appropriate. In block 405, the routine continues by registering the portable phone number and routable number combination in, for example, a database accessible by multiple service providers. In block 406, the routine takes steps to initiate activation of the new service. The routine then ends after block 406.

[0043] Figure 5 is a flow diagram 500 of an example data store routine for associating a portable mobile phone number with an interchangeable routable number and a user password for implementing unauthorized port protection. In block 501, the data store routine receives a portable number input and a routable number input for a customer. In block 502, the data store routine stores the portable number/routable number combination. In block 503, the routine generates a pointer from the portable number to the identification number so that a mapping exists between the two data entries. In decision block 504, if the routine is to handle unauthorized port protection, the routine continues at block 505. Otherwise the routine ends. In block 505, the routine requests user password information. In block 506 the routine stores the user password information and generates a mapping between the user password and the previously stored portable phone number/routable number combination. The routine then ends.

[0044] Figure 6 is a flow diagram 600 of an example routine for switching mobile communication service providers given an existing portable mobile phone number that is protected from unauthorized porting. As with the routine of Figure 4, this routine can take place at the service provider or, alternatively, at a third party number portability administrator computer. In block 601, the routine receives a request to switch service providers for a designated customer. This request may be received from a service provider contacted by the customer or, in some cases, directly from the customer. In decision block 602, the routine checks to see whether unauthorized port protection is activated for the customer. If unauthorized port protection has been activated, the routine continues at block 603. If, however, the customer has not activated unauthorized port protection, the

routine skips to block 604. In decision block 603, the routine seeks customer authorization for the service provider switch. For example, the customer may have already provided a password to a system accessible by the routine. Alternatively, a message may be sent to the customer on his or her mobile device requesting authorization of the switch. If customer authorization has been received, the routine continues at block 604. Otherwise, the routine continues at block 606 where the routine generates a denied port request notification and then ends. If, however, the correct customer authorization is received, the routine continues at block 604 where the routine registers a new mapping between the customer's permanent portable phone number and a routable number compatible with the new service provider's telephone network. In block 605, the routine generates an accept port request notification. Also in block 605, the routine may take steps to initiate cancellation of the old service and/or activation of the new service. The routine then ends.

[0045] Figure 7 is a flow diagram 700 of an example routine 700 for associating an already assigned portable phone number with a new interchangeable routable number when the portable phone number is protected from unauthorized porting in accordance with one embodiment of the invention.

[0046] In block 701, the routine receives a new mapping request based on an already assigned portable phone number/routable number combination. In block 702, the routine looks up the portable number in the data store. In decision block 703, the routine checks if the customer has requested internal port protection. If, in decision block 703, internal port protection is in place, the routine continues at decision block 704. If internal port protection is not in place, the routine continues at block 705 where the routine stores the new routable number and replaces the mapping between the portable number and the old routable number with a mapping between the portable number and the new routable number. Once this occurs, the routine performs a port success notification in block 706 and then ends. In decision block 704, the routine checks if the port has been authorized. If the port has been authorized, the routine continues at blocks 705 and 706, as

discussed above: If, however, the port has not been authorized, the routine continues at block 707 where the routine performs a port failure notification before ending.

[0047] Figure 8 is a flow diagram 800 of an example routine for authorizing a port request for a portable phone number that is protected from unauthorized porting using a password system. In this example, the routine is performed at the old service provider. In block 801, the routine receives a password for a port request. This password can be obtained directly from the customer or from a new service provider who received the password from the customer. In decision block 802, the routine checks if the password matches the password stored in the customer data record. If, there is no match for the password in the customer data record, the routine continues at block 803 where a deny port request notification is generated and sent to the requesting party before the routine ends. Otherwise, if there is a match with the password in the customer data record, the routine continues at block 804 where the routine generates and sends an accept port notification to the requesting party. At block 805, the routine then cancels the existing service of the user.

[0048] With the example routine of Figure 8, it is the new service provider's responsibility to update the mapping between the portable phone number of the customer and a new routable number that is compatible with the new service provider's system. The new service provider may do so by contacting a third party portable number administrator and providing the accept port request notification produced by the routine of Figure 8. The third party administrator may then perform a routine for mapping the portable number with the new compatible routable number in the number portability database. An example of such a routine is shown in Figure 6. Alternatively, the authorized port request routine of Figure 6 may include transferring permission to write to a portability number database from the old service provider to the new service provider.

[0049] Figure 9 is a flow diagram 900 of an example routine for obtaining authorization from a customer wishing to switch service providers when

unauthorized port protection in place. The routine may be performed in a wireless service provider system or at a third party administrator system. In block 901, the routine receives a port request from a potential new service provider. In block 902, the routine requests customer authorization by, for example, sending a request port authorization message (e.g., text message, voicemail, email, etc.) to the customer or placing an automated call to the customer. In decision block 903, if the routine receives authorization from the customer (e.g., receipt of a response to the sent authorization request message), the routine continues at block 904 where the routine returns an accept port request and ends. If, however, the customer does not authorize the port within, for example, a given time period, the routine returns a deny port request, as shown in block 905. The routine then ends.

[0050] A variation of some of the authorization techniques described above includes allowing the customer to switch service providers using, for example, an online form via the Internet. Provided that the authenticity of the online form can be verified, the party or system seeking customer authorization for a port request can use an indication of the verified online form as authorization for the switch. In this way, the customer does not have to take further steps in order to authorize such a switch.

[0051] Unless the context clearly requires otherwise, throughout the description and the claims the words "comprise," "comprising," and the like are to be construed in an inclusive sense, as opposed to an exclusive or exhaustive sense, and can be interpreted as "including, but not limited to." Words using the singular or plural number also include the plural or singular number, respectively. Additionally, the words "herein," "above," "below," and words of similar import, when used in this application, shall refer to this application as a whole and not to any particular portions of this application. When the claims use the word "or" in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list, and any combination of the items in the list.

[0052] The above detailed descriptions of embodiments of the invention are not intended to be exhaustive or to limit the invention to the precise form disclosed above. While specific embodiments of, and examples for, the invention are described above for illustrative purposes, various equivalent modifications are possible within the scope of the invention, as those skilled in the relevant art will recognize. For example, while steps are presented in a given order, alternative embodiments may perform routines having steps in a different order. The teachings of the invention provided herein can be applied to other systems, not necessarily the wireless telephone system described in detail herein. These and other changes can be made to the invention in light of the detailed description. Moreover, the elements and acts of the various embodiments described above can be combined to provide further embodiments.

[0053] In general, the terms used in the following claims should not be construed to limit the invention to the specific embodiments disclosed in the specification, unless the above detailed description explicitly defines such terms. Accordingly, the actual scope of the invention encompasses the disclosed embodiments and all equivalent ways of practicing or implementing the invention under the claims.

[0054] While certain aspects of the invention are presented below in certain claim forms, the inventors contemplate the various aspects of the invention in any number of claim forms. For example, while only one aspect of the invention is recited as embodied in a computer-readable medium (e.g., RAM or ROM memory, CD-ROM, DVD, hard drive, etc.), other aspects may likewise be embodied in a computer-readable medium. Accordingly, the inventors reserve the right to add additional claims after filing the application to pursue such additional claim forms for other aspects of the invention.